Federal Emergency Management Agency

Information Technology Architecture

Volume 1

Version 1.0

November 2, 1998

This page intentionally left blank

FEMA 332998

Federal Emergency Management Agency

Information Technology Architecture

Volume 1

November 2, 1998

Version 1.0

Prepared by:

Federal Emergency Management Agency
Information Technology Services (ITS) Directorate
500 C Street, S.W.
Washington, D.C. 20472

This page intentionally left blank

Table of Contents

List of Figures

List of Tables

List of Appendices

Foreword

This document is the Federal Emergency Management Agency's (FEMA's) initial *Information Technology (IT) Architecture* prepared under *the Information Technology Management Reform Act (ITMRA)* with the supporting guidance of OMB Memorandum M-97-16.

The document is written to be primarily directive in nature to identify and define common high-level IT architectural standards and components that can be reused across FEMA systems.

Assumptions and Constraints. The following are the basic assumptions and constraints:

- **Unclassified operations only.** To make this document accessible to the widest possible audience, the initial *IT Architecture* was developed and defined for unclassified operations only. It is anticipated that future revisions to the *FEMA IT Architecture* will have a classified annex. In related activity, FEMA is in the process of developing plans, policies, and security architecture components in response to the Critical Infrastructure Protection (CIP) program under Presidential Decision Directive 63 (PDD-63).

- **Status of business function allocation.** In developing the *FEMA IT Architecture*, over 500 highly detailed FEMA business functions for FEMA's Directorates and Administrations, Divisions, and Branches currently documented in FEMA's *Missions and Functions Manual* were reviewed and considered. Nearly all of the business functions were determined to be information technology significant to some degree.

- **Need to Conduct Business Case Analysis.** An important constraint to note is that some of the architectural components and technology may not make sound business sense given the current state of FEMA networks. For example, advanced groupware technologies such as intelligent collaboration and visualization of very large GIS data sets; integrated voice, video, and data applications; distributed interactive simulation (DIS); and distance learning (incorporating virtual reality technology) are widely accepted to be bandwidth intensive in large-scale distributed operations. The current FEMA network has limited capability to support some of these advanced technologies. Accordingly, it is important to realize that this *FEMA IT Architecture* merely provides an architectural framework for discussing how FEMA IT systems might be structured to use common architectural components that are of potential interest across a number of FEMA business units. Business case analyses for some of the more demanding architectural components clearly need to be accomplished before any actual implementation.

- **A Snapshot in time.** It was assumed that business process re-engineering (BPR) was beyond the scope of this initial *FEMA IT Architecture*. Within FEMA, improvement efforts and re-organization are in process. The *FEMA IT Architecture* will be updated as reorganizations of various parts of the Agency occur or as business processes in the Agency are re-engineered. This *FEMA IT Architecture* will encourage the enterprise-wide adoption of common architectural components, wherever possible. It sets the stage for development of an integrated IT investment strategy with detailed cost-benefit analyses for selected procurements.

- **Large requirement for enterprise information flow and many program-centric systems.** Another important consideration in the development of this initial *FEMA IT Architecture* is that over 100 FEMA organizational entities have business associations

with well over 200 other external agencies, activities, and partners. Most of these interactions were also determined to be IT significant. Further complicating the analysis was the identification of a comparatively large number of standalone program-centric legacy systems and document and data stores within the various FEMA groups. These legacy systems and document/data stores present challenges for future enterprise-wide IT integration. The analysis clearly pointed to the need for universally accepted standards to achieve information exchange and interoperability among heterogeneous systems.

With the large number of IT-significant business functions, the large number of associated IT systems and data stores, and the large number of internal and external collaborating organizations, this initial *IT Architecture* document addresses the business functions at a high-level. For each business function, FEMA can provide additional supporting details, if required. FEMA has started development of an *IT Architecture* Data Base to identify and address architecture components for all of the business functions. Future revisions to this document and the development of the ancillary electronic *IT Architecture* Data Base (described in Section 1.12.1) should help address business functions, information flows, systems/applications, and data stores at progressively finer levels of detail in future revisions to this document.

Use of Terminology. Within the context of the directive tone noted above, the following terms have these meanings:

- The use of the term ***shall*** implies that the statement is mandatory for compliance in the development of future IT systems or for systems that are proposed to be re-engineered. Requests for waivers must be justified and require formal action by the FEMA Information Resources Board (IRB) in accordance with the provisions contained in Section 4 of this document.

- The use of the term ***will*** implies an intent to consider the requirement in earnest in the development of future IT systems or systems that are proposed to be re-engineered. In general, *IT Architecture* requirements characterized as *will* can be expected to have viable alternatives. In the interest of architectural standardization, proposed systems that do not comply with a *will* requirement must also request a waiver, but the burden-of-proof will not be as stringent.

- The use of the terms ***must***, ***is declared to be***, or ***is determined to be*** should be interpreted in the same sense as the term *shall*.

- The use of the terms ***may***, ***might***, ***could, should*** is intended to be only advisory in nature. At some point in the future, the architectural requirement may be tightened to *will* or *shall* status. There is no requirement to request a waiver or deviation from these standards from the IRB for future IT systems or those proposed to be re-engineered. However, the waiver must be noted in the systems development documentation and must be addressed as appropriate in systems engineering reviews.

Within the Technical Reference Model (Section 2), the following terms have the meaning as indicated:

- ***Adopted*** means that the standard or standard tool has been formally accepted by the CIO for the service area or architectural component to which it refers.

- ***Under evaluation*** means that the standard or standard tool has not yet been formally accepted and is being actively evaluated or considered within FEMA.

- ***Suggested*** is a less strong term than *under evaluation*. *Suggested* really means that there is a potential opportunity for technology insertion or standardization that ought to be more formally considered – business case and funding permitting.

- ***In-service use*** means that the standard or tool is currently being used within FEMA IT systems. It is subject to re-evaluation, re-engineering, or additional development prior to being formally adopted.

Mandatory Compliance Statement. This *FEMA IT Architecture* is mandatory for compliance on the development of new IT systems and any proposed re-engineering, re-hosting, or additional development of legacy systems. Section 4 provides amplifying information.

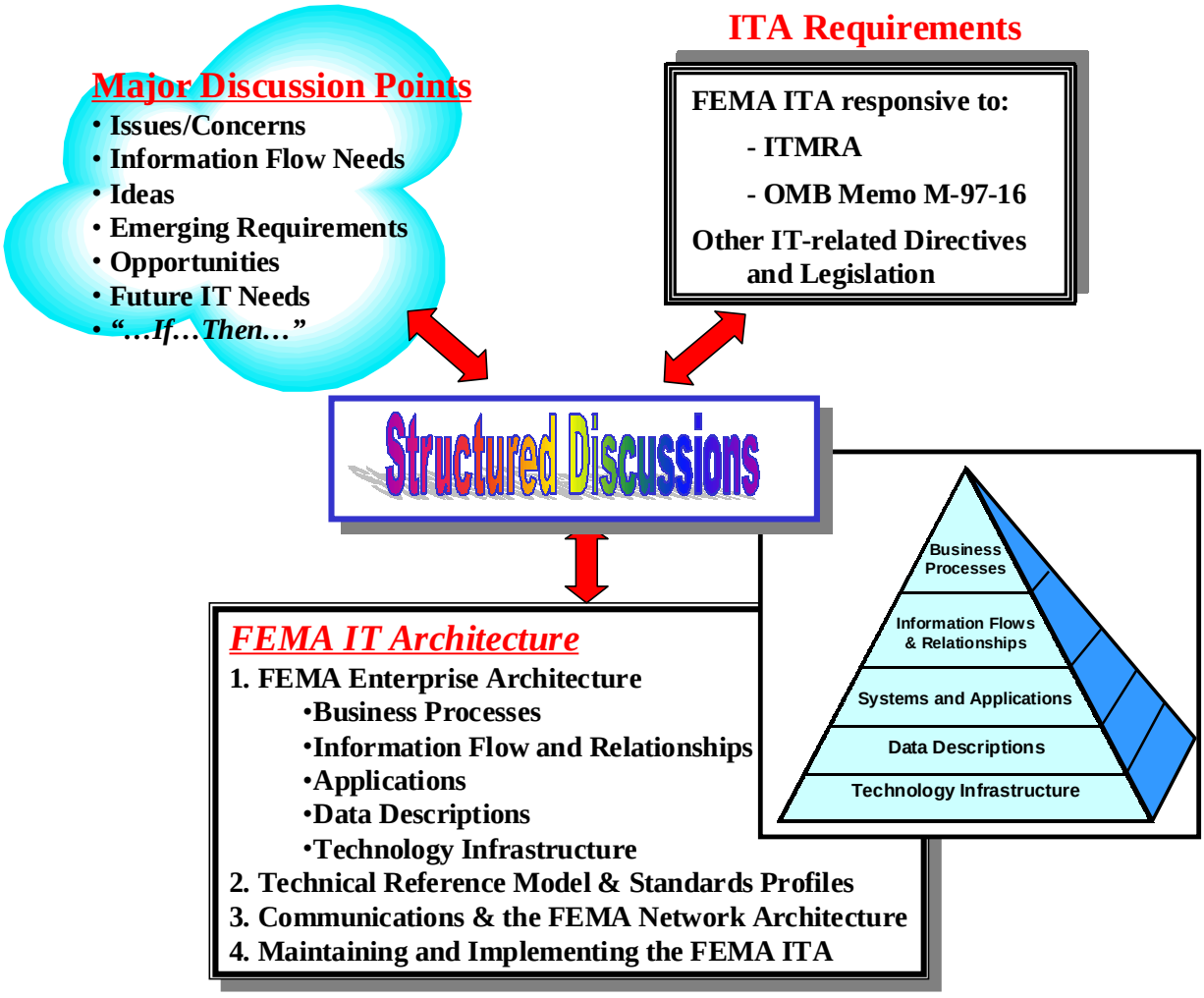
Point of Contact. The point of contact for questions or comments regarding this *FEMA IT Architecture* is G. Clay Hollister, FEMA Chief Information Officer (CIO), at (202) 646-3006. His e-mail address is Clay.Hollister@fema.gov.

This page intentionally left blank

Executive Summary

Introduction. The Federal Emergency Management Agency (FEMA) is the Federal governmental unit that bears primary responsibilities for the nation's emergency management system. When devastation is serious and exceeds the capability and resources of local and State governments to respond, States turn to the Federal government for help and assistance. Once the President has declared a major disaster or emergency, FEMA coordinates not only its own response activities but also those of as many as 27 other Federal agencies.

Methodology and Approach. This document is FEMA's initial *IT Architecture*. As illustrated below, the *Architecture* was developed through a series of structured discussions across FEMA Headquarters and Regional staff. The structured discussions mirrored the architectural *pyramid* implied by OMB Memorandum M-97-16. This *IT Architecture* document closely follows that approach.



As the length of the discussions permitted, the following architectural components were addressed:

- **Business functions**
- **Subactivities**

- **Inputs and outputs**
- **Operational environmental factors**
- **Systems and applications**
- **Documents and data stores**
- **Technologies and security components**.

The results of these discussions led to the development of the target *FEMA IT Architecture* with the following major characteristics:

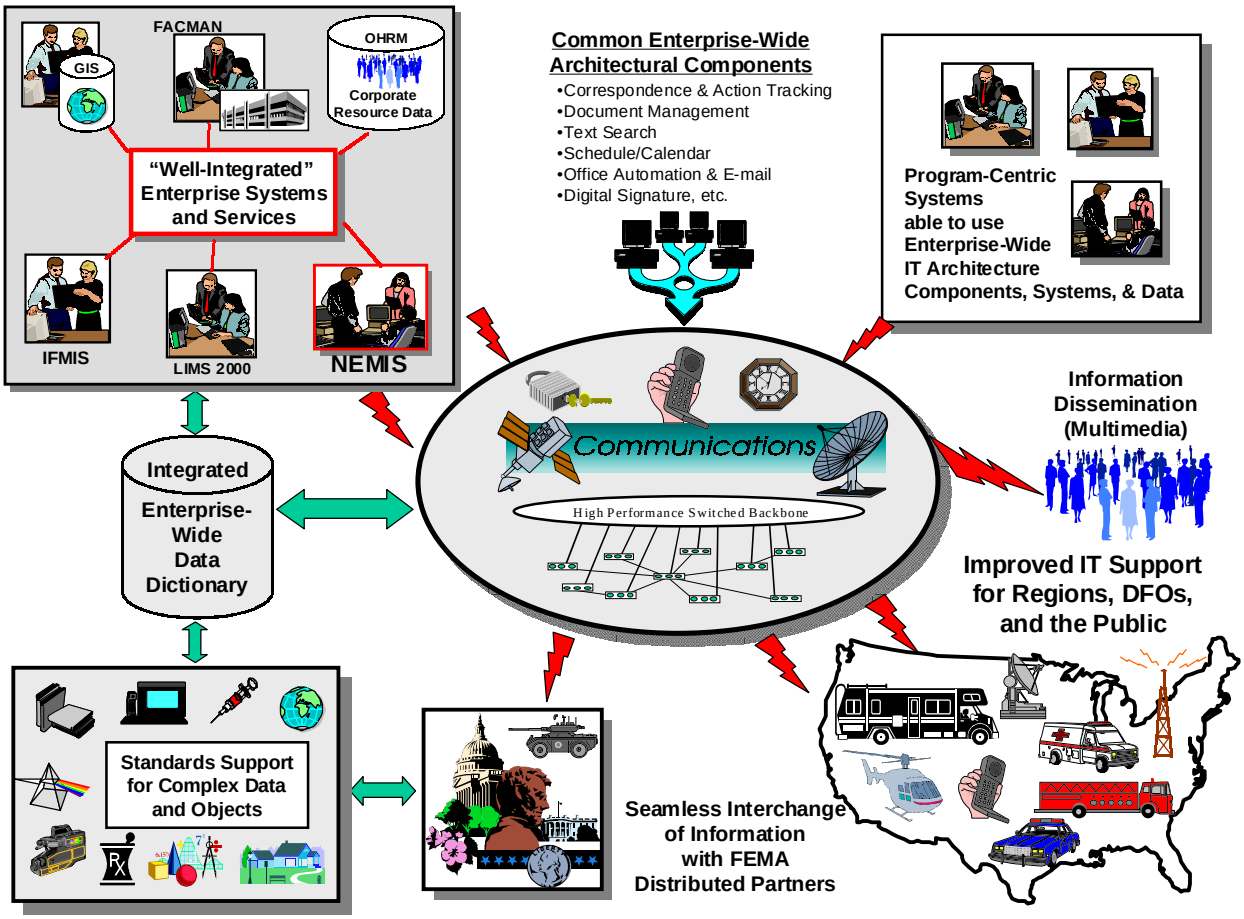
- **Well-integrated enterprise-wide systems and services**
- **Improved communications and networking**
- **Consideration of impact on legacy telecommunications systems as new capability is added**
- **Adequate bandwidth for advanced IT applications**
- **Potential for increased connectivity**
- **Achieving a consensus on standards across the enterprise**
- **Engineering concerns addressed**
- **Emphasis on open systems standards**
- **Improved data integrity over the life cycle**.

Because of FEMA's significant investment in the National Emergency Management Information System (NEMIS), this target *FEMA IT Architecture* has designated NEMIS as an IT architectural *cornerstone*. Within FEMA, NEMIS is the lead system for providing comprehensive mission support, interoperability, and re-use. NEMIS is a proving ground for implementing advanced IT concepts. While NEMIS is an architectural *cornerstone*, the *FEMA IT Architecture* is open to good ideas and innovation from any enterprise-wide system. This *FEMA IT Architecture* considers such IT concepts as:

- Developing integrated enterprise-wide systems and services and a common data dictionary.
- Developing common and re-usable enterprise-wide IT architectural components based on open systems approaches that can be used by both enterprise-wide and program-centric systems.
- Developing, re-engineering, consolidating, and re-hosting selected program-centric systems to be compliant with the architecture and the enterprise-wide data dictionary.
- Providing an enterprise approach for systems engineering and configuration management.
- Enhancing the FEMA communications backbone to provide improved IT support and improved Quality of Service to the Regions, Disaster Field Offices (DFOs), and the public.
- Exploring the potential for improved connectivity with FEMA's business partners, Regions, States, and local government through establishment of Extranets and Virtual Private Networks (VPNs).
- Achieving consensus on approaches for creating, managing, using, and interchanging complex documents and data sets in an intelligent manner across the enterprise.
- Performing technology insertion in such areas as digital libraries, distributed collaboration tools, distance learning, interactive GIS, secure electronic commerce, virtual reality, simulation, and other emerging technologies as added IT support to FEMA business processes.

As a matter of high priority and in response to Presidential Decision Directive 63 (PDD-63), the FEMA CIO, in the role of FEMA's Chief Information Assurance Officer (CIAO), is currently in the process of developing a comprehensive plan for protecting FEMA's critical IT systems and networks. This *IT Architecture* is consistent with that direction and firmly establishes and validates many of the underlying operational requirements of the Critical Information Protection (CIP) program.

FEMA Information Systems Landscape. The target *FEMA IT Architecture* is depicted in the following graphic.



This page intentionally left blank

Page Down